

REMARKS

Claims 1 to 3 were pending in the application at the time of examination. Claims 1 to 3 stand rejected as obvious.

Claims 1 to 3 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Application Publication No. 2002/0184507, hereinafter referred to as Makower, in view of U.S. Patent Application Publication No. 2002/0067832, herein after referred to as Jablon.

In continuing to cite to Makower, the rejection stated "Applicant's arguments . . . do not clearly point out the patentable novelty . . . they do not show how the amendments avoid such references or objections." Applicants respectfully disagree. Applicants explicitly pointed out defects in the rejection that did not comply with the requirements of the MPEP. Since the MPEP requirements were not met, a prima facie obviousness rejection was not established.

The MPEP requires:

When applying 35 U.S.C. 103, the following tenets of patent law must be adhered to:

(A) The claimed invention must be considered as a whole;

(B) The references must be considered as a whole and must suggest the desirability and thus the obviousness of making the combination;

(C) The references must be viewed without the benefit of impermissible hindsight vision afforded by the claimed invention; and

(D) Reasonable expectation of success is the standard with which obviousness is determined.

MPEP § 2141, 8th Ed. Rev. 3, p. 2100-125 (August 2005).

The language in this section of the MPEP is mandatory. Thus, failure to comply with any one of the four requirements means that a prima facie obviousness rejection has not been made and Applicants' Claim 1 is therefore patentable.

With respect to the requirement that the claimed invention must be considered as a whole, the MPEP further directs:

To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). "All words in a claim must be considered in judging the patentability of that claim against the prior art."

MPEP § 2141.03, 8th Ed. Rev. 3, p. 2100-149 (August 2005).

The rejection failed to consider the first element of Claim 1 as a whole. The first element of Claim 1 is quoted below. In this quote, the information in italics is part of the claim that was quoted in the rejection. The text that is shown with strike-through has been moved in the rejection and reinserted as shown by the underlined text in italics. The text in bold was not considered in the rejection of the first element.

obtaining a user identifier, said user identifier comprising an identification server ID and an ~~identification randomized ID~~, said identification server ID identifying an identification server peer group, said identification server peer group comprising at least one server that maintains a mapping between an identification randomized ID and an identification randomized ID and a user authentication peer group capable of authenticating a user associated with a particular identification randomized ID, and a mapping between said identification randomized ID and user information;

Because the text in bold was not considered, the claim was not considered as whole. The rejection has failed to even allege any teaching of two peer groups, an identification server peer group and a user authentication peer group. Accordingly, a *prima facie* obviousness rejection has not been made in view of the above quotations from the MPEP.

Further, Claim 1 recites in part:

said user identifier comprising an identification server ID and an identification randomized ID

Thus, Claim 1 defines that a user identifier includes an identification server ID and an identification randomized ID.

The rejection stated:

. . . Makower discloses . . . obtaining a user identifier, said user identifier comprising an identification server, said identification server ID identifying an identification server peer group, said identification server peer group comprising at least one server that maintains a mapping between an identification randomized ID (Makower teaches a federation of servers that each server has an associated identifier, that uniquely distinguishes it from all other server), [see Makower, section 0023 and 0028] and an identification randomized ID (Makower teaches that when data is received at the web server from the client, the web server creates a unique, random string called a challenge), [see Makower, section 0028];

The rejection only quotes Applicants' claim language and cites no suggestion or teaching in Makower of obtaining a user identification. The rejection cites to the pieces included in the user identification, the identification server ID and the identification randomized ID, but fails to cite any teaching or suggestion in Makower that the two are included in a user ID. Thus, the rejection has failed to establish any teaching of obtaining any user identifier, and has failed to cite any teaching of the specific user identifier recited in Claim 1. Thus, Applicants have shown at multiple levels that at best only the gist of the claim has been considered and not explicit claim limitations. Again, the MPEP directs:

Distilling an invention down to the "gist" or "thrust" of an invention disregards the requirement of analyzing the subject matter "as a whole."

MPEP § 2141.02 II, 8th Ed. Rev. 3, p. 2100-130 (August 2005).

The above facts alone are sufficient to overcome the obviousness rejection of Claim 1.

However, Claim 1 further recites:

said identification server peer group comprising

[1] at least one server that maintains a mapping between an identification randomized ID and a user authentication peer group capable of authenticating a user associated with a particular identification randomized ID, and

[2] a mapping between said identification randomized ID and user information

Thus, the identification server peer group has two features [1], [2] that are recited in Claim 1. As noted above, a portion of the first feature [1] was not even considered and so this alone is sufficient to overcome the rejection. However, the rejection cited paragraph [0028] of Makower as suggesting the second feature [2] and part of the first feature [1]. The features cited in the rejection are associated with a web server 20 of Makower.

As previously noted,

Makower taught that there are two possibilities for authentication that are determined by a central server: (1) the client browser is not recognized by the central server; and (2) the client browser is recognized by the central server.

Specifically, Makower first taught:

. . . if the central sign-on server 32 does not recognize the client browser 42 via a cookie, the central sign-on server 32 creates a cookie with a new, unique value (step 404). Additionally, the central sign-on server 32 creates an entry on a local

table located on the central sign-on 32 server using the newly created cookie and the web server 20 server identification as a concatenated primary key (step 406). The central sign-on server 32 then redirects the client browser 42 back to the web server 20 (step 410). . . .

Makower, Paragraph [0031]

. . . .

Thus, if the authentication is not provided by the central server upon finding the cookie, a routine log-in is used by the web server to make the authentication. There is no teaching of any mapping associated with the authentication.

The rejection has failed to establish that web server 20 maintains a mapping between an identification randomized ID and a user authentication peer group capable of authenticating a user associated with a particular identification randomized ID as required by Claim 1.

Since the central server performs authentication as quoted above, to read on the first feature [1] quoted above from Claim 1 with respect to a user authentication peer group, the mapping would have to be between the challenge (which was identified in the rejection as the identification randomized ID) and the central server. However, the challenge is associated with "the operative federation identification of the web server 20." The rejection has failed to show that there is any mapping between the challenge and the central server. .

Applicants note that the rejection combined another reference with Makower. However, this reference was directed only at the second paragraph of Claim 1. Thus, assuming the combination of references is correct, the information in the secondary reference does not cure the defects of the primary reference as noted above with respect to the first paragraph of Claim 1. Applicants request reconsideration and withdrawal of

the obviousness rejection of Claim 1 in view of Makower taken with Jablon.

Claim 2 is a program storage device corresponding to method Claim 1 and thus includes substantially the same distinctive feature as Claim 1. Claim 3 is a means-plus-function claim corresponding to method Claim 1 and thus includes substantially the same distinctive feature as Claim 1. Accordingly, the above comments with respect to Claim 1 are incorporated herein by reference for Claims 2 and 3. Applicants request reconsideration and withdrawal of the obviousness rejection of each of Claims 2 and 3 of Makower taken with Jablon.

Claims 1 to 3 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,706,427, hereinafter referred to as Tabuki, in view of U.S. Patent Application Publication No. 2002/0067832, herein after referred to as Jablon.. The Examiner stated, in part (emphasis in original):

. . . Tabuki discloses a *method for enhanced quality of identification in a data communication network* (Tabuki teaches in summary a method for authenticating users on networks that includes an application server that requests a user host to send authentication data to a verification server) [see Tabuki, abstract, Col. 2, lines 24-39], *the method comprising: obtaining a user identifier, said user identifier comprising an identification server ID (verification server name)* (Tabuki teaches utilizing a Sys Uniq Key which is a system key assigned to each user, and is unique in the verification server's table. As well as utilizing the user's Sys Uniq Key, the system of Tabuki further teaches this key is utilize [Sic] in combination with the verification server name), [see Tabuki, Col. 5, lines 30-60 and Col. 6, lines 23-27], *said identification server ID identifying an identification server peer group* (Tabuki further teaches utilizing the verification server's name in addition to the Sys Uniq key when there is a plurality of different verification servers), [see Tabuki, Col. 6, lines 4-38],

However, Tabuki taught:

Therefore, strictly speaking, identification of the user is made on the basis of the combination of Sys Uniq Key and verification server name.

Tabuki, Col. 6, lines 25 to 27.

Thus, while the Examiner has again equated the identification server peer group of Claim 1 with the combination of Tabuki's verification server name and the Sys Uniq key, Tabuki's verification server name, either alone or in combination with a Sys Uniq key, does not identify an identification server peer group. Rather, the combination of verification server name and Sys Uniq key in Tabuki, as quoted above, uniquely identifies a user where multiple verification servers are used. Applicants respectfully submit that teaching using a verification server name and a Sys Uniq key to identify a particular user when there is more than one verification server fails to suggest or disclose an ID that identifies an identification server peer group.

The rejection continued:

. . . (Tabuki teaches that a verification servers have an internal database with identification data and valid authentication data of user hosts (user authentication peer group)), [see Tabuki, Col. 4, lines 22-35, Col. 5, lines 21-38]; . . . *configured to search for one or more matching entries* (Tabuki teaches that authentication data of the user is sent to a verification server, in which the verification server matches authentication data of the user by searching within a relational database), [see Tabuki, Col. 3, lines 5-22 and Col. 4, lines 33-45]

Thus, the rejection admits that a verification server, or server group includes both the identification and authentication functions.

As interpreted by the rejection, Tabuki teaches a method for authenticating users on a network where a verification server performs *both* identification and authentication

functions. In contrast, Claim 1 recites an *identification* server peer group to perform identification functions and a separate user *authentication* peer group to perform user authentication functions. Thus, the rejection itself shows that Tabuki teaches away for the two server groups as recited in Claim 1. The MPEP stated:

A *prima facie* case of obviousness may also be rebutted by showing that the art, in any material respect, teaches away from the claimed invention.

MPEP §2144.05 III, Eighth Ed., Rev. 3, p. 2100-149 (August 2005)

The Examiner next stated (Emphasis in original):

. . . Tabuki does not explicitly disclose an identification randomized Id and a mapping between an identification randomized ID and a user authentication peer group capable of authenticating a user associated with a particular randomized ID, and a mapping between said identification randomized ID and user information.

. . . Jablon discloses (e.g., systems, methods and software for remote password authentication using multiple servers). [Sic] Jablon discloses an *identification randomized Id and a mapping between an identification randomized ID and a user authentication peer group capable of authenticating a user associated with a particular randomized ID, and a mapping between said identification randomized ID and user information* [see Jablon, section 0092,0015].

Applicants first note that even if the rejection's interpretation of Jablon is correct and the combination of references is correct, the additional information does not overcome the deficiencies of the primary reference as noted above. Therefore, Claim 1 distinguishes over the combination of references.

Further, Applicants respectfully submit that the rejection mischaracterized Jablon. Jablon taught a way for a user to

develop a secret master key using information from a plurality of authentication servers. Specifically,

[0079] An exemplary system in accordance with the present invention comprises one or more clients and a plurality of authentication servers coupled together by way of a network. In the exemplary system, a client uses Modified SPEKE to retrieve a share Ki of a secret master key from each authentication server, where i is a variable that designates the specific server. The client combines the respective shares from each of the servers to create the master key Km, which is used to authenticate to the servers, and to retrieve and decrypt sensitive data (including her private key) that is stored securely on the servers or elsewhere.

The rejection has not cited any teaching that the share Ki is used in any mapping. Moreover, the Ki is associated with the client and not to identify the server. In addition, Paragraph 92, described a "forgiving system," in which the user is forgiven for access attempts. Specifically, Paragraph 91 provides the context for paragraph 92,

[0091] Using the forgiveness protocol, a user's honest mistakes are forgiven. Alice sends evidence of her recent prior invalid access attempts in a request for forgiveness after each successful authentication. Upon receiving and validating this evidence, each server erases the mistake from the record, or records the event as a corrected forgivable mistake. By fine-tuning a server's event log in this manner, a system administrator gets a more detailed view of when the system is truly at risk, as opposed to when valid users are merely being frustrated.

Paragraph 92 describes how the operations of paragraph 91 are accomplished. Forgiving past erroneous access attempts is unrelated to the interplay of identification and authentication peer groups as recited in Claim 1.

Applicants have demonstrated that cited portions of the primary reference fail to teach or suggest several aspects of Applicants' invention, and the secondary reference fails to

teach or suggest elements of Applicants' invention. Any one of these showing is sufficient to overcome the obviousness rejection of Claim 1. Accordingly, Applicants request reconsideration and withdrawal of the obviousness rejection of Claim 1 in view of Tabuki taken with Jablon.

Claim 2 is a program storage device corresponding to method Claim 1 and thus includes substantially the same distinctive feature as Claim 1. Claim 3 is a means-plus-function claim corresponding to method Claim 1 and thus includes substantially the same distinctive feature as Claim 1.

Accordingly, the above comments with respect to Claim 1 are incorporated herein by reference for Claims 2 and 3.

Applicants request reconsideration and withdrawal of the obviousness rejection of each of Claims 2 and 3 in view of Tabuki taken with Jablon.

Claims 1 to 3 remain in the application. For the foregoing reasons, Applicant(s) respectfully request allowance of all pending claims. If the Examiner has any questions relating to the above, the Examiner is respectfully requested to telephone the undersigned Attorney for Applicant(s).

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on December 8, 2005.



Attorney for Applicant(s)

December 8, 2005
Date of Signature

Respectfully submitted,



Forrest Gunnison
Attorney for Applicant(s)
Reg. No. 32,899
Tel.: (831) 655-0880